**Step 1: Sign in to the AWS Management Console**

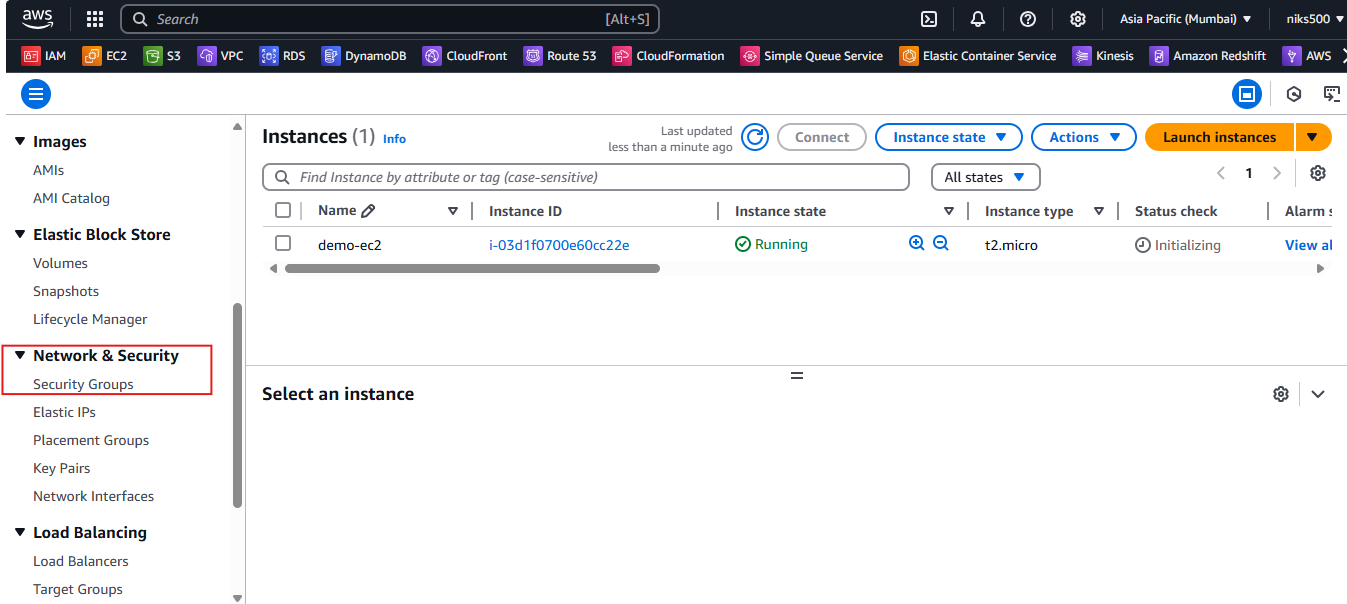
* Navigate to the [AWS Management Console](https://aws.amazon.com/console/) and log in with your credentials.

**Step 2: Go to the EC2 Dashboard**

* In the **Search bar**, type **EC2** and select **EC2** from the Services list.

**Step 3: Access Security Groups**

* On the left-hand side, under **Network & Security**, click on **Security Groups**.



**Step 4: Create a New Security Group**

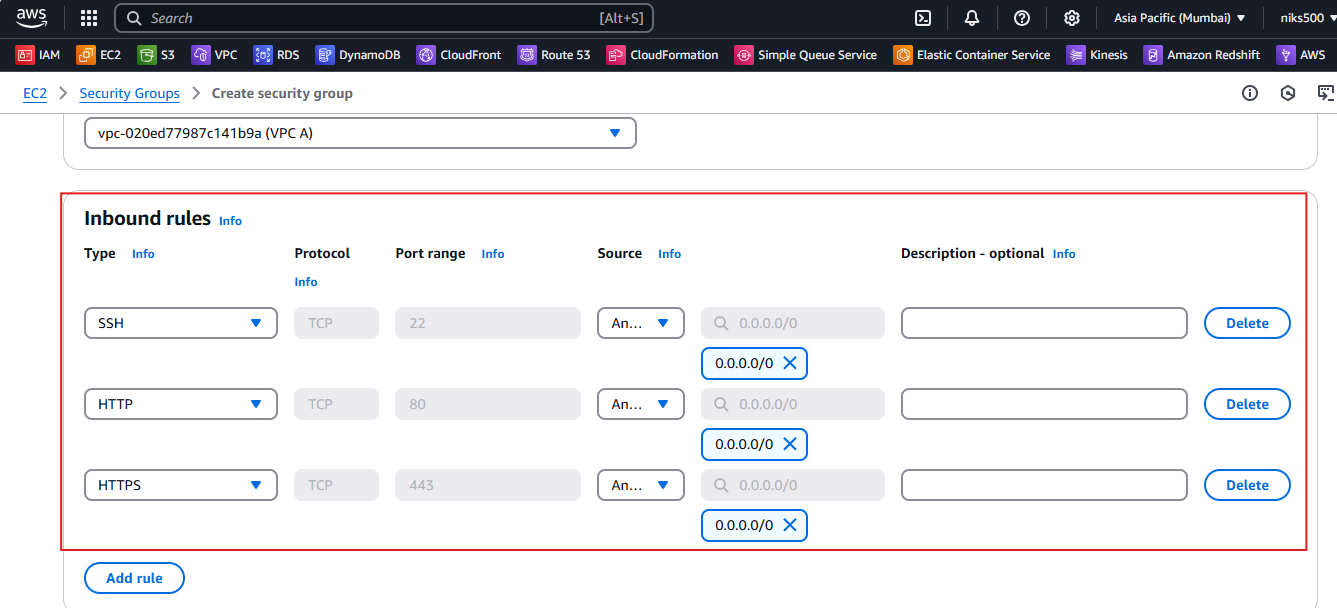
* Click the **Create security group** button at the top.

**Step 5: Configure the Security Group**

* **Name the Security Group:**  
  Choose a descriptive name (e.g., MyWebServerSG).
* **Description:**  
  Provide a brief description (e.g., Security group for web servers).
* **VPC:**  
  Select the **VPC** where your EC2 instance will reside (or use the default VPC).

**Step 6: Add Inbound Rules**

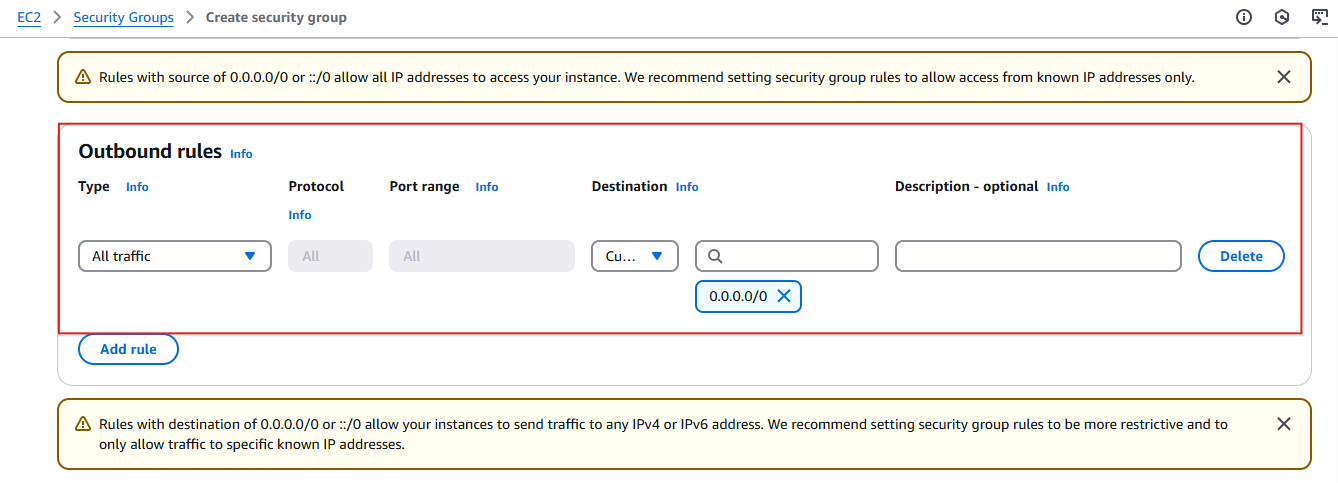
* In the **Inbound rules** section, click **Add Rule** to specify allowed traffic.
  + **SSH (Port 22)** – For Linux instances, use this rule to allow SSH access from your IP address.
    - **Type:** SSH
    - **Protocol:** TCP
    - **Port Range:** 22
    - **Source:** Choose "My IP" for your current IP address or specify a range.
  + **HTTP (Port 80)** – For web servers, add this to allow traffic on port 80.
    - **Type:** HTTP
    - **Protocol:** TCP
    - **Port Range:** 80
    - **Source:** Anywhere (0.0.0.0/0) or specify trusted IPs for more security.
  + **HTTPS (Port 443)** – For secure web servers, add this to allow traffic on port 443.
    - **Type:** HTTPS
    - **Protocol:** TCP
    - **Port Range:** 443
    - **Source:** Anywhere (0.0.0.0/0) or trusted IP ranges.
  + **Custom Ports** – You can add more specific ports based on your requirements (e.g., MySQL, RDP for Windows).



**Note:** Be cautious with the **Source** setting; avoid setting it to "Anywhere" (0.0.0.0/0) unless necessary for public access, as it opens your server to the world.

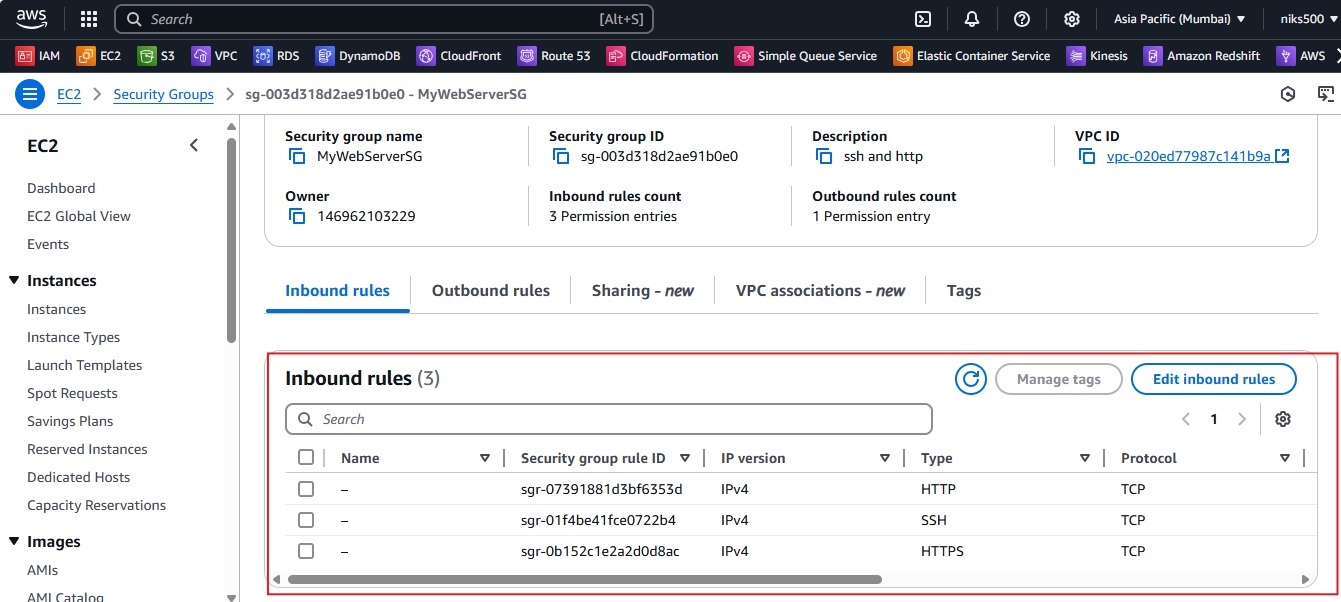
**Step 7: Add Outbound Rules**

* By default, a security group allows all outbound traffic. You can leave this as it is unless you need to restrict outbound traffic.
  + **Type:** All Traffic
  + **Protocol:** All Traffic
  + **Port Range:** All traffic
  + **Destination:** Anywhere (0.0.0.0/0)



**Step 8: Review and Create**

* **Review the settings** to ensure everything is configured correctly.
* Click **Create security group** to save and create your security group.



**Step 9: Attach Security Group to an EC2 Instance**

* After creating the security group, you can attach it to your EC2 instance when launching it or modify the security group for an existing instance.
  + To modify an existing EC2 instance, go to the **Instances** section in EC2.
  + Select the instance you want to modify.
  + Under **Security** in the bottom panel, click on **Security Groups** and then **Edit**.
  + Choose your newly created security group and click **Save**.

